IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Application No. :

U.S. National Serial No. :

Filed :

PCT International Application No. : PCT/FR2003/003309

VERIFICATION OF A TRANSLATION

I, Charles Edward SITCH BA,

Deputy Managing Director of RWS Group Ltd UK Translation Division, of Europa House, Marsham Way, Gerrards Cross, Buckinghamshire, England declare:

That the translator responsible for the attached translation is knowledgeable in the French language in which the below identified international application was filed, and that, to the best of RWS Group Ltd knowledge and belief, the English translation of the amended sheets of the international application No. PCT/FR2003/003309 is a true and complete translation of the amended sheets of the above identified international application as filed.

I hereby declare that all the statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the patent application issued thereon.

Date: April 26, 2005

Signature :

For and on behalf of RWS Group Ltd

Post Office Address : Europa House, Marsham Way,
Gerrards Cross, Buckinghamshire,
England.

CLAIMS

1. A method for analyzing the security of an information system comprising:

- a modeling phase (1, 2), comprising on the one hand the specification (1) of the architecture of the information system with a graphical representation of a set of components of the system and relations between said components, each component being associated with at least one state initialized with a sound value, the relations between two determined components comprising propagation relations able to convey attacks, and on the other hand the specification (2) of a set of behavioral rules, from the standpoint of the operation of the system and from the standpoint of security, associated with the components of the system, each behavioral rule comprising one or more predicates and/or one or more actions; and,

- a simulation phase, comprising the specification (3) and the simulation (4) of potential attacks against the information system, a successful attack causing a state of a component to pass to an unsound value.

2. The method as claimed in claim 1, according to which, a name being associated with each component, one or more adjectives may also be associated with said component, which adjectives make it possible to designate said component without naming it.

3. The method as claimed in claim 1 or claim 2, according to which determined states are associated with each component of the information system, each state being able to take a sound value and one or more unsound values.

4. The method as claimed in claim 3, according to which certain at least of said states pertain respectively to the activity, the confidentiality, the

integrity and/or the availability of the component with which they are associated.

5. The method as claimed in any one of the previous claims, according to which an alleged name may be associated with any determined component, in particular in the case where said determined component is a usurper.

6. The method as claimed in any one of the previous claims, according to which a link to another component may be associated with any determined component, in particular in the case where said determined component is usurped and where said other component is a usurper.

7. The method as claimed in any one of the previous claims, according to which the propagation relations are bidirectional relations able to convey attacks in both directions.

8. The method as claimed in any one of the previous claims, according to which the relations between any two determined components comprise service relations making it possible to designate a component on the basis of another component.

9. The method as claimed in any one of the previous claims, according to which the behavioral rules comprise rules for propagating attacks, these rules being for example implemented in components which are vectors of attacks, and rules for absorbing attacks, these rules being for example implemented in components which are the target of attacks.

10. The method as claimed in any one of the preceding claims, according to which the behavioral rules comprise binary rules, for example Boolean logic conditions giving a value of type yes/no, and/or functional rules, for example logic conditions

involving a routing action (for a propagation rule) or contagion action (for an absorption rule).

11. The method as claimed in any one of the preceding claims comprising, at the end of the modeling phase (Figure 3), the construction (35) of a local routing table, making it possible to direct an attack from a start component to a finish component.

12. The method as claimed in claim 11, according to which the local routing table is generated automatically according to the principle of the shortest path between the start component and the finish component.

13. The method as claimed in any one of claims 3 to 12, according to which the attacks simulation step comprises the updating of the state of a component of the system altered by a successful attack.

14. The method as claimed in claim 13, according to which the simulation phase furthermore comprises the building of a file or journal of the attacks, containing the log of the changes of the state of the components consequent upon successful attacks, in particular to allow subsequent processing by a user.

15. The method as claimed in any one of the preceding claims, according to which the attacks comprise elementary attacks corresponding to unsound state values.

16. The method as claimed in any one of the preceding claims, according to which the attacks furthermore comprise a special usurping attack.

17. The method as claimed in any one of the preceding claims, according to which an attack is defined, in particular, by a type of attack, a type of protocol,

and attack path elements.

18. The method as claimed in claim 17, according to which the attack path elements comprise a start component, a finish component, a target component, and as appropriate one or more intermediate components.

19. The method as claimed in claim 17 or claim 18, according to which the list of components already traversed by an attack is saved in at least one or more upstream stacks.

20. The method as claimed in claim 19, according to which the upstream stacks comprise a stack (110) containing the exhaustive list of all the components traversed, designated by their real name.

21. The method as claimed in claim 19 or claim 20, according to which the upstream stacks comprise a stack (120) containing the list of only those components traversed which are opaque, designated by their real name or, as appropriate, by their alleged name.

22. The method as claimed in any one of claims 17 to 21, according to which the list of destination components of an attack is saved in at least one downstream stack (130).

23. The method as claimed in any one of the preceding claims, according to which the attacks are defined in a language using the same words as a language in which the behavioral rules are defined.

24. The method as claimed in any one of the preceding claims, according to which the modeling phase and/or the simulation phase are implemented by a user by means of a man/machine interface comprising a multiview functionality, according to which a graphical representation of the system is presented to the user

as several views.

25. The method as claimed in claim 24, according to which each view represents a subsystem of the system, which is relatively autonomous and independent of the remainder of the system.

26. The method as claimed in claim 24 or claim 25, according to which the function of interconnection between the components included in two distinct views is ensured only via the common component or the common components shared by the two views.

27. The method as claimed in any one of claims 24 to 26, according to which the behavioral rules for the components belonging to a view do not call by name upon components belonging to another view.

28. The method as claimed in any one of claims 24 to 27, according to which the views are associated with respective subsystems, for example of like level, which are interconnected together via at least one common component.

29. The method as claimed in any one of claims 24 to 27, according to which a higher view is associated with the system as a whole, whereas one or more lower views are respectively associated with a determined subsystem of the system.

30. The method as claimed in claim 29, according to which a determined component, common to the higher view and to a determined lower view, represents the corresponding subsystem viewed from the system as a whole, and vice versa.

31. The method as claimed in claim 30, according to which said common component is the sole interface between the higher view and said determined lower view.

32. The method as claimed in any one of the preceding claims, according to which the modeling phase furthermore comprises the specification of one or more basic metrics associated respectively with the components.

33. The method as claimed in claim 32, according to which the basic metrics comprise, a metric of effectiveness of parries, a metric of effectiveness of detection of attacks, and/or a metric of the means of an attacker.

34. The method as claimed in any one of the preceding claims, according to which the simulation phase comprises the calculation of one or more metrics of probability of mishap.

35. The method as claimed in claim 34, according to which the metrics of probability of mishap comprise a metric of probability of passage of an attack on a component.

36. The method as claimed in claims 32 and 34, according to which the metric of probability of passage of an attack on a component is calculated according to the formula "probability of passage = (means of the attacker)/(effectiveness of the protection)".

37. The method as claimed in claim 34, according to which the metrics of probability of mishap comprise a metric of probability of nondetection of an attack on a component.

38. The method as claimed in claims 33 and 37, according to which the metric of probability of nondetection of an attack on a component is calculated according to the formula "probability of nondetection = (means of the attacker)/(effectiveness of the

detection)".

39. A device for the implementation of the method as claimed in any one of the preceding claims, comprising a man/machine interface (15) for the implementation of the modeling phase and/or an attacks/parries engine (16) for the implementation of the simulation phase.

40. The device as claimed in claim 39, in which the man/machine interface exhibits a functionality of multiview display of the system modeled.

41. The device as claimed in claim 39 or claim 40, in which the man/machine interface makes it possible to display the system modeled according to a components/relations model.